UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

STEVEN LINTHICUM, individually and on behalf of all others similarly situated, Plaintiff v. LASTPASS US LP, Defendant	)	Case No. **CLASS ACTION COMPLAINT** **[JURY TRIAL DEMANDED]**

Plaintiff Steven Linthicum ("Plaintiff" or "Mr. Linthicum"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), through his undersigned counsel, brings this action against defendant LastPass US LP, ("LastPass" or "Defendant"), based upon personal knowledge and, upon information and belief, including from his counsel's investigation. Mr. Linthicum seeks monetary damages, injunctive relief, and/or all appropriate equitable remedies.

I. NATURE OF THE ACTION

1. This class action arises out of a 2022 data breach ("Data Breach") at LastPass, which sells subscription-based password management services to both individuals and businesses. LastPass identifies itself as a "pioneer in cloud security technology," and a provider of "award-winning password and identity management solutions that are convenient, effortless, and easy to manage." [1] LastPass markets its service to internet users, including plaintiff and Class Members, seeking additional security and protection for their private and valuable passwords.

[1] "About LastPass," https://www.lastpass.com/company/about-us (last accessed on March 5, 2023).

LastPass offers a solution to these consumers, including Plaintiff and Class Members, to store all of their login credentials and passwords in a LastPass "vault," for which they need to remember only one "master password."

2. Indeed, Section 4.2 of LastPass' Terms of Service for Personal Users states that LastPass "ha[s] implemented and maintain[s] appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."

3. LastPass touts its own success, claiming over 33 million customers and over 100,000 businesses secure their passwords with LastPass, and numerous awards from cybersecurity experts:

4. Although Last Pass offers to essentially sell security, it does not provide robust protections for its users' data.

5. LastPass recognized in a press release that the Data Breach began sometime before August 25, 2022, but has failed to provide an exact date or precise details about the security failure.

6. On August 25, 2022, LastPass CEO Karim Toubba notified customers via a blog post that two weeks earlier the corporation experienced a Data Breach in its "development environment"—where LastPass designs customer-facing virtual environments before deployment. In that same notice, LastPass explicitly averred that customers' "Master

Passwords"—the master key to unlock vaults containing hidden passwords to customers' online accounts and PII—remained uncompromised. [2] In response, LastPass recommended that customers take no action. [3]

7. On September 15, 2022, LastPass again confirmed there was no evidence that the Data Breach involved access to customer data or password vaults. This despite admitting that its investigation into the mechanics of the initial Data Breach were "inconclusive" and that the cyber attacker had had "persistent access" such that they could "impersonate" a LastPass employee-developer and thereby access the development environment. [4]

8. Two and a half months later, on November 30, 2022, LastPass acknowledged "unusual activity within a third-party cloud storage service" shared by LastPass and its affiliate, GoTo. LastPass contradicted its earlier assurances to customers in admitting that the August 2022 Data Breach had allowed a cyber attacker to gain access to customer information. [5]

9. Finally, on December 22, 2022, more than four months after the Data Breach began, LastPass notified customers of the ongoing nature of the Data Breach and admitted the cyberattacker stole sensitive customer PII, including customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass

---

[2] LastPass, "Notice of Recent Security Incident" from August 25, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[3] *Id*.

[4] LastPass, "Notice of Recent Security Incident" from September 15, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[5] LastPass, "Notice of Recent Security Incident" from November 30, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

service. Further, LastPass admitted that customer vault data was stolen.

10. Stunningly, LastPass again provided no assistance to customers aside from a "password settings and best practices" guide that predated and was arguably neutered by the monthslong, intervening customer Data Breach, and recommended customers self-audit to determine their own compliance with the suggestions. And for those customers whose passwords do not comply with the suggestions, LastPass recommended customers "consider" individually changing passwords for each website they have visited and stored—websites which, for Plaintiff and Class Members, range in the multiple hundreds.

11. LastPass grossly mismanaged the Data Breach and failed to protect customers, while keeping them in the dark.

12. LastPass failed to meaningfully notify customers about the breach for several months. And they have still not confirmed when it occurred, how much data was taken, and what they will do to provide remedies to customers who have suffered losses as a result of their failed security.

13. Plaintiff brings this class action on behalf of all similarly situated consumers harmed by the 2022 Data Breach, asserts claims of negligence, breach of contract/breach of the implied covenant of good faith and fair dealing, breach of implied contract, unjust enrichment, breach of fiduciary duty, violation of California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq.*, violation of California Customer Records Act ("CCRA") Cal. Civ. Code § 1798.80 *et seq.*, and seeks compensatory damages, including restitution and disgorgement, punitive damages, declaratory and injunctive relief, and attorneys' fees.

II. PARTIES

A. Plaintiff

14. Plaintiff, Steven Linthicum, brings this action on behalf of himself and those similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, LastPass, through its actions described herein, leaked, disbursed, and furnished Plaintiff's and Class Members' valuable PII to unknown cybercriminals, causing them present, immediate, imminent, and continuing increased risk of harm.

15. Plaintiff is a resident of Oceanside, California, and resided in California during the entire period that Plaintiff was a customer and subscriber of LastPass.

16. Plaintiff is a cybersecurity professor, Certified Information Systems Security Professional (CISSP), and Certified Cloud Security Professional (CCSP).

17. Plaintiff has maintained a LastPass account since 2009. In the last three years, Plaintiff purchased annual subscriptions for LastPass Premium on February 25, 2021, February 25, 2022, and February 25, 2023.

18. Plaintiff stored approximately three hundred (300) distinct login credentials in his LastPass account.

19. Plaintiff's name, e-mail address, social security number, and login credentials for his bank account were included in the login credentials saved in his LastPass account.

20. Plaintiff's saved billing information for LastPass also included his name, credit card number, email address, physical address, and telephone number.

21. Plaintiff's master password had over 24 characters, in compliance with LastPass' best practices for password management.

22. Despite the fact that Plaintiff is a savvy cybersecurity professional, Plaintiff learned about the LastPass Data Breach not from LastPass directly, but from a cybersecurity

industry podcast. LastPass did not notify its users that their PII was no longer secure.

23. Since the announcement of the Data Breach, Plaintiff has spent significant time changing the login credentials, including passwords, for the approximately 300 accounts that he used LastPass's service to secure.

24. Plaintiff did not receive the benefit of his bargain and expected security that LastPass touted throughout its marketing materials. Plaintiff is disappointed with how LastPass "attempted to mask the Data Breach." Due to these concerns, Plaintiff has decided to use another password management service provider, BitWarden, which he views as more secure than LastPass since the LastPass Data Breach. Though Plaintiff intended to use BitWarden exclusively for his secure password management needs, he was unable to cancel his LastPass subscription before it automatically renewed in February of 2023. Even so, Plaintiff intends to refrain from further use or patronage of LastPass due to its mismanagement of the 2022 Data Breach.

B. Defendant

25. Defendant LastPass is a limited partnership organized under the laws of Delaware, with its principal place of business at 333 Summer Street Boston, Massachusetts, 02210.

26. LastPass is a password management services company.

III. JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because at least one member of the Class, as defined below, is a citizen of a different state than LastPass.

28. This Court has personal jurisdiction over LastPass because LastPass maintains its

principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

29. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because the Defendant's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

IV. FACTUAL ALLEGATIONS

A. LastPass and Its Privacy and Data Security Representations

30. LastPass is a self-described "password manager tool" that promises customers can "secure every account with one, simple login." [6] The service LastPass offers to provide paying customers is security. Specifically, the corporation sells its customers two main services: (1) creating, safeguarding, and deploying "strong, unique" passwords, and (2) acting as a virtual master key for customers to use to access their various internet accounts across devices and with a single sign-in. Passwords created for specific online sites are stored by LastPass in virtual "password vaults," which LastPass maintains are only accessible to customers who use their "master password." Additionally, LastPass offers customers the ability to store payment information in a digital wallet and provides "dark web monitoring" that includes monitoring third-party data breaches of customer accounts, thereby promising to keep customers "informed and secure."[7]

31. In addition to touting itself as being a "secure" method for storing customer

[6] LastPass, "What is a password manager?," https://www.lastpass.com/password-manager (last accessed March 6, 2023).

[7] *Id*.

passwords, LastPass promises to provide customers "more" by storing customers' personal information, filling online forms with customers' financial and accounting information, and "securely" sharing access to customers' accounts.[8] LastPass encourages customers to entrust the corporation with highly sensitive Personal Identifiable Information (PII) and sensitive documents, promising that all will be held "securely."[9] Indeed, LastPass explicitly promises to safeguard customers' "most valuable documents," including passports, credit cards, and social security information.[10]

32. The corporation represents to customers, including to Plaintiff and Class Members, that PII stored on LastPass will remain protected and confidential, that customers have ultimate control over access to the PII stored on LastPass, and that LastPass will proactively and affirmatively ensure customer PII remains secure from exposure.

33. Indeed, Section 4.2 of LastPass' Terms of Service for Personal Users states that LastPass "ha[s] implemented and maintain[s] appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."[11]

34. The company assures customers that their "data is kept secret, even from us"[12] and that "[o]nly you can unlock [your vault] with your master password."[13] Indeed, LastPass

---

[8] LastPass, "What is a password manager?," https://www.lastpass.com/password-manager (last accessed March 6, 2023).

[9] *Id*.

[10] *Id*.

[11] LastPass, "Terms of Service" https://www.lastpass.com/legal-center/terms-of-service/personal (last accessed March 6, 2023).

[12] LastPass, "Why LastPass?" https://www.lastpass.com/security/zero-knowledge-security (last accessed March 6, 2023).

[13] *Id*.

goes as far as stating customers may, in using LastPass, "make it nearly impossible for hackers to access your accounts." [14]

35. LastPass trots out multiple figures in support of its guarantee that it provides customers "stringent security measures, continuous, future-oriented improvements, and clear communication," including that over 33 million customers and over 100,000 businesses secure their passwords with LastPass, and that it has received numerous awards from cybersecurity experts: [15]

36. LastPass lulls customers into a sense of calm that the corporation will proactively and affirmatively secure customer PII. It styles these services as "auto-pilot for all your passwords" that provides "peace of mind everywhere you go" [16] and assures customers that "[s]afeguarding your data is what we do, with proactive security and reliability as cornerstones of our mission." [17] While LastPass makes clear that customers, including Plaintiff and Class Members, "can trust it with [their] sensitive data," the company further affirms that in the event

[14] LastPass, "Why LastPass?" https://www.lastpass.com/security/zero-knowledge-security (last accessed March 6, 2023).

[15] LastPass, "Security Architecture," https://www.lastpass.com/security (last accessed March 6, 2023).

[16] LastPass, "Password management from anywhere," https://www.lastpass.com (last accessed March 6, 2023).

[17] LastPass, "Security Architecture," https://www.lastpass.com/security/zero-knowledge-security (last accessed March 6, 2023).

of a vulnerability, such as a data breach, the LastPass team "reacts swiftly" and "communicates transparently with our community." [18]

37. LastPass knows that the customer PII entrusted to it is highly sensitive and highly valuable to hackers. Regarding banking, the corporation stated that "extra precautions are essential when it comes to protecting [customers'] money." [19] The corporation called email the "hub" of online life and the "gateway" to preforming password resets, admonishing that customers "need to protect it." [20] LastPass admits that social media sites contain personal information that "hackers love." [21]

38. In acknowledgement of the value of PII to its customers and to potential hackers, LastPass makes a "pledge" to its customers, including that it will protect customer data by making security its "top priority," communicate with customers regarding "security-related incident[s]," and that its services will be "effortless to manage." [22]

B. The Data Breach

39. On August 25, 2022, LastPass CEO Karim Toubba notified customers via a blog post that two weeks earlier the corporation experienced a Data Breach in its "development environment"—where LastPass designs customer-facing virtual environments before

[18] *Id*.

[19] LastPass, "What is a password manager?," https://www.lastpass.com/password-manager (last accessed March 6, 2023).

[20] *Id*.

[21] *Id*.

[22] LastPass, "Security Architecture," https://www.lastpass.com/security (last accessed March 6, 2023).

deployment.[23] LastPass assured customers that, after investigating the Data Breach, it had seen "no evidence that this incident involved any access to customer data or encrypted password vaults."[24] It determined that the hacker gained access to portions of the LastPass development environment through a compromised employee developer account, taking with them "portions of source code and some propriety technical information." [25] The corporation assured customers that "products and services are operating normally" and LastPass saw "no further evidence of unauthorized activity." [26]

40. In that same notice, LastPass explicitly averred that customers' "Master Passwords"—the master key to unlock vaults containing hidden passwords to customers' online accounts and PII—remained uncompromised. [27] LastPass further claimed that no data within customers' vaults and no personal information had been compromised, and that the corporation's security measures continued to "ensure[ ] that only the customer has access to decrypt vault data."[28] Notably, in response to its own question, "What should I do to protect myself and my vault data?", LastPass answered: "At this time, we don't recommend any action on behalf of our users or administrators." [29] Customers who sought more information beyond the blog post were met with the statement that LastPass would "continue to update [its] customers with the

[23] LastPass, "Notice of Recent Security Incident" from August 25, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[24] *Id*.

[25] *Id*.

[26] *Id*.

[27] LastPass, "Notice of Recent Security Incident" from August 25, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[28] *Id*.

[29] *Id*.

transparency they deserve." [30]

41. Nearly three weeks later, on September 15, 2022, LastPass posted another blog notice to customers in order to, in its own words, provide "peace-of-mind to our consumer and business communities." [31] At this point, LastPass revealed that the Data Breach had occurred over a four-day period in August 2022 and that the "LastPass security team detected the threat actor's activity and then contained the incident." [32] LastPass again confirmed there was no evidence that the Data Breach involved access to customer data or password vaults. LastPass made this assurance despite admitting that its investigations into the mechanics of the initial Data Breach were "inconclusive" and that the cyber attacker had had "persistent access" such that they could "impersonate" a LastPass employee-developer and thereby access the development environment. [33] Indeed, despite this, LastPass explicitly assured customers that their "data and passwords are safe in our care." [34]

42. For two and a half months customers held to the assurance that their data and passwords were safe in the care of LastPass, until November 30, 2022, when CEO Karim Toubba notified customers in a blog post that the August 2022 Data Breach had spawned more problems with security. [35] LastPass acknowledged "unusual activity within a third-party cloud storage

---

[30] *Id*.

[31] LastPass, "Notice of Recent Security Incident" from September 15, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[32] *Id*.

[33] *Id*.

[34] LastPass, "Notice of Recent Security Incident" from September 15, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[35] LastPass, "Notice of Recent Security Incident" from November 30, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6,

service" shared by LastPass and its affiliate, GoTo. LastPass contradicted its earlier assurances to customers in admitting that the August 2022 Data Breach had allowed a cyber attacker to gain access to customer information. [36] Nevertheless, LastPass again mouthed the refrain: "customers' passwords remain safely encrypted." [37] Except for providing a link to its long-published recommended best practices page, LastPass provided no further guidance about how to respond to the spread of the ongoing Data Breach. [38]

43. Finally, on December 22, 2022, more than four months after the Data Breach began, LastPass CEO Karim Toubba notified customers of the ongoing nature of the Data Breach and admitted the cyberattacker stole sensitive customer PII. [39] LastPass stated that using a "cloud storage access key and dual storage container decryption keys" obtained in the Data Breach, the cyberattacker copied customer PII "from backup." [40] As a result of the Data Breach, LastPass admits exposure of "customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service." [41] LastPass explained that [t]he threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a proprietary binary format that contains both unencrypted data, such

---

2023).

[36] *Id*.

[37] *Id*.

[38] *Id*.

[39] LastPass, "Notice of Recent Security Incident" from December 22, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

[40] *Id*.

[41] LastPass, "Notice of Recent Security Incident" from December 22, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed March 6, 2023).

as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data." [42]

44. Though LastPass admitted that portions of *un*encrypted customer PII had already been exposed in the Data Breach, the corporation maintains that customers' exposed, *encrypted* PII data "remain secured" due to the fact that, according to LastPass, such information "can only be decrypted with a unique encryption key derived from each user's master password . . ." [43] However, this supposed assurance of security is undercut by the fact that, as LastPass admitted to customers, "[t]he threat actor may attempt to use brute force to guess [a customer's] master password and decrypt copies of vault data they took" or "target customers with phishing attacks, credential stuffing, or other brute force attacks against online accounts associated with [a customer's] LastPass vault." [44]

45. Without elaborating on the extent of customers affected by the Data Breach, LastPass offered customers paltry help. It again trotted out a "password settings and best practices" guide that predated and was arguably neutered by the monthslong, intervening customer Data Breach, and recommended customers self-audit to determine their own compliance with the suggestions. And for those customers whose passwords do not comply with the suggestions, LastPass recommended customers "consider" individually changing passwords for each website they have visited and stored[45]—websites which, for Plaintiff and Class Members, range in the multiple hundreds.

C. LastPass Caused Plaintiff and Class Members Actual, Concrete,

[42] *Id*.

[43] *Id*.

[44] *Id*.

[45] *Id*.

Preventable Harm

46. As a result of the Data Breach, Plaintiff and millions of Class Members have suffered and will continue to suffer concrete and actual harm. LastPass promised to safeguard Plaintiff's and Class Members' sensitive PII, including passwords securing highly sensitive accounts. As a result of the Data Breach, Plaintiff's and Class Member's sensitive PII was compromised, unlawfully accessed, and made subject to unlawful use by cybercriminals.

47. In addition to initially failing to deliver on its promise to maintain Plaintiff's and Class Member's PII data safely and securely prior to the Data Breach—by, for example, ensuring proper company security protocols were in place and ensuring customers hewed to consequential security standards—LastPass's gross mismanagement made a bad breach worse.

48. LastPass failed to give adequate notice to customers about the extent and severity of the Data Breach in real time (or even near real time). In a wide-ranging Data Breach that spanned nearly five months, LastPass provided four communications to customers, only two of which made clear that customer data was exposed. As a result, Plaintiff and Class Members were left in the dark about whether and to what extent sensitive PII was exposed. Further, Plaintiff and Class Members were unable to make informed decisions about seeking to mitigate harm resulting from the Data Breach, such as by procuring credit reporting services to assist in the detection of fraud or purchasing password management services from other companies.

49. Due to LastPass's missteps, Plaintiff and Class Members were forced to resort to self-help to mitigate the risk of secondary harms resulting from the Data Breach, including themselves engaging in the very service for which LastPass was contracted to provide: secure password management services. Plaintiff and Class Members were left with no choice but to individually change passwords to multiple hundreds of websites to reduce the risk of harms

resulting from the LastPass Data Breach. Additionally, Plaintiff and Class Members contracted with other password management service providers to ensure efficient security in the long term.

50. In this, Plaintiff and Class Members lost money, time, and the peace of mind that LastPass was meant to afford all along.

51. Plaintiff and Class Members face imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the Data Breach and LastPass's deceptive and unconscionable conduct.

D. Effects of the Data Breach

52. It is well known that PII is a highly valued commodity and a frequent target of hackers. Here, the failure of Last Pass to deliver the promised and paid-for security left Plaintiff and Class Members vulnerable, exposing their most private and valuable accounts to third party access.

53. PII is such a valuable commodity to identity thieves that, once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

54. Thus, Plaintiff and Class Members must vigilantly monitor their credit reports, financial accounts, and other areas of concern for the foreseeable future.

55. There may be a significant time lag between when PII is stolen and when it is actually misused.

56. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[46]

[46] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007),

57. LastPass has offered Plaintiff and Class Members no solution and not even any assistance to guard against the risks they face after LastPass failed to secure their valuable information.

58. As the result of the Data Breach, Plaintiff and Class Members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. identity theft and fraud resulting from theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;

c. losing the inherent value of their PII;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized access to and misuse of their online accounts;

f. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

g. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including

https://www.gao.gov/assets/gao-07-737.pdf (last visited March 5, 2023)

discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

h. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in LastPass's possession and is subject to further breaches so long as LastPass fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

59. Additionally, Plaintiff and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[47]

60. One study on website privacy determined that U.S. consumers valued the

[47] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited March 5, 2021).

restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[48] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be much higher today.

V. CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action on his own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "Class Members."

62. Pursuant to Fed. R. Civ. P. 23, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class:** All natural persons residing in the United States whose PII was compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **California Subclass**: All individuals within the State of California whose PII and/or financial information was exposed to unauthorized third parties as a result of the Data Breach discovered by Defendant in August 2022.

63. Excluded from the Class and Subclasses are LastPass' officers, directors, and employees; any entity in which LastPass has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of LastPass. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

[48] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17, Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited March 5, 2021).

64. **Numerosity.** The members of the Class (and Subclasses) are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on LastPass' own statements, the Class consists of over 33 million persons whose data was compromised in the Data Breach, who can be identified by reviewing the PII exfiltrated from Last Pass' databases.

65. **Commonality.** There are questions of law and fact common to Plaintiff and Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether LastPass' data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether LastPass' data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards and best practices;

c. Whether LastPass properly implemented its purported security measures to protect Plaintiff's and the Class's PII from unauthorized capture, dissemination, and misuse;

d. Whether LastPass took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether LastPass disclosed Plaintiff's and the Class's PII in violation of the understanding that the PII was being disclosed in confidence and should be maintained;

f. Whether LastPass willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's PII;

g. Whether LastPass was negligent in failing to properly secure and protect Plaintiff's and the Class's PII; and

i. Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

66. **Typicality.** Plaintiff's claims are typical of those of the Class Members because Plaintiff's PII, like that of every Class Member, was compromised in the Data Breach.

67. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of Class Members, including those from states and jurisdictions where he does not reside. Plaintiff's Counsel are competent and experienced in litigating class actions and have been appointed lead counsel by many different courts in many other class action suits.

68. **Predominance.** LastPass has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data at issue here was secured by LastPass and accessed during the Data Breach. The common issues arising from LastPass' conduct affecting Class Members, as described supra, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

69. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claim is prohibitively high and

would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for LastPass. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

70. **Injunctive Relief is Appropriate.** LastPass has failed to take actions to safeguard Plaintiff's and Class Members' PII such that injunctive relief is appropriate and necessary. LastPass has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On behalf of the Nationwide Class and the California Subclass)

71. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

72. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, inter alia, to act with reasonable care to secure and safeguard their PII and financial information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII and financial information of Plaintiff and Class Members in their computer systems and on their networks. These common law duties existed because Mr. Linthicum and Class Members were the foreseeable and probable victims of any

inadequate security practices in LastPass's affirmative development and maintenance of its data security systems.

73. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in their possession;

b. to protect Plaintiff's and Class Members' PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to act on warnings about data breaches timely; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII and financial information.

74. Defendant knew that the PII and financial information were private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

75. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and financial information, the vulnerabilities of their data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

76. Defendant knew, or should have known, that their data systems and networks did

not adequately safeguard Plaintiff's and Class Members' PII and financial information.

77. Only Defendant was in the position to ensure that their systems and protocols were sufficient to protect the PII and financial information that Plaintiff and Class Members had entrusted to them.

78. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiff and Class Members.

79. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII and financial information contained therein.

80. Plaintiff's and Class Members' willingness to entrust Defendant with their PII and financial information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII and financial information they stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

81. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiff and/or Class Members.

82. Defendant breached their general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII and financial information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;

d. by failing to provide adequate supervision and oversight of the PII and financial information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PII and financial information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII and financial information;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

83. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

84. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

85. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and financial information to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and financial information.

86. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and financial information.

87. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and financial information of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' PII and financial information were accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and financial information by adopting, implementing, and maintaining appropriate security measures.

88. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

89. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

90. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by a business, such as Defendant, of failing to use reasonable measures to protect PII and financial information. The FTC publications and orders described above also form part of the basis of Defendant's duty.

91. Defendant violated 15 U.S.C. §45 by failing to use reasonable measures to protect PII and financial information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and financial information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

92. Defendant's violation of 15 U.S.C. §45 constitutes negligence per se.

93. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and financial information in their continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

94. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

95. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

COUNT II

BREACH OF CONTRACT/BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On behalf of the Nationwide Class and the California Subclass)

96. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

97. Plaintiff and Class Members entered into valid and enforceable express contracts with LastPass under which Plaintiff and Class Members agreed to provide their PII to LastPass,

and LastPass agreed to provide password and identity management services that included the implementation of adequate data security standards, protocols, and procedures to ensure the protection of Plaintiff's and Class Members' PII.

98. In every contract entered into between Plaintiff and Class Members and LastPass, including those at issue here, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as LastPass was obligated to protect (and not interfere with) the privacy and protection of Plaintiff's and Class Members' PII. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

99. To the extent LastPass' obligation to protect Plaintiff's and Class Members' PII was not explicit in those express contracts, the contracts also included implied terms requiring

100. LastPass to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII, including in accordance with trade regulations, federal, state and local laws, and industry standards. No customer would have entered into these contracts with LastPass without the understanding that their PII would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' express contracts.

101. Indeed, Section 4.2 of LastPass' Terms of Service for Personal Users states that LastPass "ha[s] implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."

102. Plaintiff and Class Members agreed, among other things, to provide their PII in

exchange for LastPass' agreement to protect the confidentiality of that PII.

103. The protection of Plaintiff's and Class Members' PII was a material aspect of Plaintiff's and Class Members' contracts with LastPass, because Plaintiff and Class Members would not have provided their PII to LastPass or allowed LastPass to control the passwords allowing access to their PII, if they had known that LastPass did not plan to provide this promised protection.

104. LastPass' promises and representations described above relating to industry standards and LastPass' purported concern about its users' privacy rights are express terms of the contracts between LastPass and its customers, including Plaintiff and Class Members. LastPass breached these promises by failing to comply with reasonable industry practices.

105. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by LastPass and/or otherwise understood that LastPass would protect its customers' PII if that information were provided to LastPass.

106. Plaintiff and Class Members fully performed their obligations under their contracts with LastPass; however, LastPass did not.

107. As a result of LastPass' breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with LastPass; losing the difference in the value between the services with adequate data security that LastPass promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to change multiple account passwords, the master password, and monitor accounts. Additionally, Plaintiff and Class Members have been put at increased risk of future fraud and/or misuse of their PII, which may

take years to manifest, discover, and detect.

108. As a direct and proximate result of LastPass' breach of the implied covenant of good faith and fair dealing, Plaintiff and the Class Members have suffered injury and are entitled to damages, including restitution, unjust enrichment and disgorgement in an amount to be proven at trial, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III

BREACH OF IMPLIED CONTRACT

(On behalf of the Nationwide Class and the California Subclass)

109. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

110. Plaintiff brings this claim alternatively to his claim for breach of contract.

111. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class. Defendant required Plaintiff and Class Members to provide and entrust their PII and financial information as a condition of obtaining Defendant's services.

112. Defendant solicited and invited Plaintiff and Class Members to provide their PII and financial information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII and financial information to Defendant.

113. As a condition of their relationship with Defendant, Plaintiff and Class Members provided and entrusted their PII and financial information to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

114. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII and financial information to Defendant, in exchange for, amongst other things, the protection of their PII and financial information.

115. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

116. Defendant breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect their PII and financial information and by failing to provide timely and accurate notice to them that their PII and financial information was compromised as a result of the Data Breach.

117. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and the impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web, (e) lost work time and (f) other economic and non-economic harm. Members' PII and financial information.

COUNT IV

UNJUST ENRICHMENT

(On behalf of the Nationwide Class and the California Subclass)

118. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

119. Plaintiff brings this Count under California Law individually and on behalf of the Nationwide Class and/or California Subclass ("Class") against Defendant.

120. By their wrongful acts and omissions described herein, Defendant have obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

121. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PII and financial information to Defendant for the purpose of obtaining services, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PII and financial information secure.

122. Defendants were aware, or should have been aware, that reasonable consumers would have wanted their PII and financial information kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

123. Defendant was also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, they would negatively affect Plaintiff's and Class Members' decision to seek services therefrom.

124. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Plaintiff and Class Members.

125. Defendant was unjustly enriched at the expense of Plaintiff and Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and

Class Members. By contrast, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or services that did not satisfy the purposes for which they bought/sought them.

126. Since Defendants' profits, benefits and other compensation were obtained by improper means, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

127. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits, or other compensation obtained by Defendant from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

COUNT V

BREACH OF FIDUCIARY DUTY

(On Behalf of the Nationwide Class and the California Subclass)

128. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

129. Plaintiff and Class Members have an interest, both equitable and legal, in the PII that was conveyed to and collected, stored, and maintained by LastPass and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach. LastPass, in taking possession of this highly sensitive information, formed a special relationship with its customers, including Plaintiff and the Class.

130. Plaintiff and the Class Members put their trust and confidence in LastPass'

131. judgment, honesty, and integrity in protecting their PII and the various accounts that could be accessed through use (or misuse) of that PII.

132. LastPass knew that Plaintiff and Class Members were relying on LastPass, and accepted this trust and confidence when it accepted PII from Plaintiff and Class Members.

133. As a result of that special relationship, LastPass was provided with and stored private and valuable information belonging to Plaintiff and the Class, which LastPass was required by law and industry standards to maintain in confidence.

134. In light of the special relationship between LastPass and Plaintiff and Class Members, whereby LastPass became a guardian of Plaintiff's and Class Members' PII, LastPass undertook a fiduciary duty to act primarily for the benefit of its customers, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' PII.

135. LastPass had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiff's and Class members' PII and to maintain the confidentiality of their PII.

136. LastPass owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

137. Plaintiff and Class Members have a privacy interest in their personal and proprietary matters and LastPass had a duty not to disclose or allow unauthorized access to such confidential information.

138. Plaintiff's and Class Members' PII is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class Members did not consent to nor authorize LastPass to release or disclose their PII to unknown criminal actors.

139. LastPass breached its fiduciary duty to Plaintiff and Class Members when

Plaintiff's and Class Members' PII was disclosed to unknown criminal hackers by way of LastPass' own acts and omissions, as alleged herein.

140. LastPass knowingly breached its fiduciary duties by failing to safeguard Plaintiff's and Class Members' PII, including by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class Members thereof;

g. failing to follow its own privacy policies and practices published to its customers;

h. storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and

i. making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PII to a criminal third party.

141. But for LastPass' wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy would not have been compromised and their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

142. As a direct and proximate result of LastPass' breach of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their PII; theft of their PII; costs associated with the detection and prevention of fraud and unauthorized use of their PII; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the LastPass' Data Breach—including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with law enforcement; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII entrusted, directly or indirectly, to LastPass with the mutual understanding that LastPass would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their PII, which remains in LastPass' possession and is subject to further breaches so long as LastPass fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their PII.

143. LastPass breached its fiduciary duty to Plaintiff and Class Members when it made an unauthorized release and disclosure of their confidential PII and, accordingly, it would be inequitable for LastPass to retain the benefits it has received at Plaintiff's and Class Members' expense.

144. Plaintiff and Class Members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200 ET SEQ.

(On Behalf of the California Subclass)

145. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

146. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

147. Defendant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff and the California Subclass Members from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendant failed to:

i. Secure its website;

ii. Secure access to its servers;

iii. Comply with industry-standard security practices;

iv. Employ adequate network segmentation;

v. Implement adequate system and event monitoring;

vi. Utilize modern payment systems that provide more security against intrusion;

vii. Install updates and patches in a timely manner, and

vii. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

c. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass Members whose PII has been compromised;

d. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 et seq., and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

e. Defendant's failure to implement and maintain reasonable security measures also led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiff and the California Subclass Members could not

know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendants caused;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the California Subclass Members' PII;

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

j. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82; and

k. Other ways to be discovered and proved at trial.

148. Defendant's representations and material omissions of fact, as alleged herein, to Plaintiff and the California Subclass Members were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the privacy of consumers' PII.

149. Defendant intended to mislead Plaintiff and the California Subclass Members and induce them to rely on their misrepresentations and material omissions of fact as alleged herein.

150. Had Defendant disclosed to Plaintiff and the California Subclass Members that their data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff and the California Subclass Members' PII as part of the services and goods Defendant provided without advising Plaintiff and the California Subclass Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff and the California Subclass Members. Accordingly, Plaintiff and the California Subclass Members acted reasonably in relying on Defendant's misrepresentations and material omissions of fact, the truth of which they could not have discovered.

151. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and the California Subclass Members' rights.

152. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and the California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

153. Plaintiff and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

154. Plaintiff and California Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all California Class Members.

COUNT VII

VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")

CAL. CIV. CODE § 1798.80 *ET SEQ.*

(On behalf of the California Subclass)

155. Plaintiff restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

156. This Count is brought on behalf of Plaintiff and the California Subclass against Defendant.

157. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

158. Each Defendant is a business that maintains PII about Plaintiff and California Subclass Members within the meaning of Cal. Civ. Code §1798.81.5.

159. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §1798.81.5, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

160. Plaintiff and California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages, civil penalties, injunctive relief, and reasonable attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Mr. Linthicum, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Last Pass as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under California Code of Civil Procedure section 382, including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class

Members;

5. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and laws;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendants from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Mr. Linthicum, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

DATED: March 6, 2023

Respectfully Submitted,

/s/ Edward F. Haber
Edward F. Haber (BBO #215620)
Michelle H. Blauner (BBO #549049)
Patrick J. Vallely (BBO #663866)
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
Telephone: (617) 439-3939
Fax: (617) 439-0134
ehaber@shulaw.com
mblauner@shulaw.com
pvallely@shulaw.com

Sabita J. Soneji (*pro hac vice* forthcoming)
Cort T. Carlson (*pro hac vice* forthcoming)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Telephone: (510) 254-6808
Facsimile: (202) 973-0950
ssoneji@tzlegal.com
ccarlson@tzlegal.com

Counsel for Plaintiff and the Proposed Class